

SMALL BUSINESS ADMINISTRATION
PRIVACY IMPACT ASSESSMENT

Name of Project: Loan Accounting System

Once the PIA is completed and the signature approval page is signed, please provide copies of the PIA to the following:

- SBA IT Security Manager
- SBA OCIO IT Portfolio Division
- SBA Privacy Act Officer

Do not email the approved PIA directly to the Office of Management and Budget email address identified on the Exhibit 300 form. One transmission will be sent by the OCIO Portfolio Management Division

Also refer to the signature approval page at the end of this document.

A. CONTACT INFORMATION:

1) Who is the person completing this document?

Glenn Hannon
Financial Analyst
Office of Financial Assistance
202-205-7507
Glenn.Hannon@sba.gov
409 3rd Street S.W.
Washington, DC 20416
(202) 205-7122

2) Who is the System Owner?

Eric Zarnikow
Associate Administrator
Office of Capital Access
Eric.Zarnikow@SBA.gov
(202) 205-6657

Jennifer Main
Chief Financial Officer
Office of the Chief Financial Office
Jennifer.Main@sba.gov
(202) 205-6449

Herbert Mitchell
Associate Administrator
Office of Disaster Assistance
Herbert.Mitchell@sba.gov
202-205-6734

Christine Liu
Chief Information Officer,
Office of the Chief Information Officer
christine.liu@sba.gov
(202) 205-6716

3) Who is the System Manager for this system or application?

Steve Kucharski
Modernization Program Manager
Office of Financial Assistance
Stephen.kucharski@sba.gov
202-205-7551

4) Who is the IT Security Manager who reviewed this document?

Dave McCauley
Chief Information Security Officer
Office of the Chief Information Officer
David.McCauley@sba.gov
202-205-7103

5) Who is the Bureau/Office Privacy Act Officer who reviewed this document?

Ethel Matthews
Senior Advisor to the Chief Privacy Officer
Office of the Chief Information Officer
Ethel.Matthews@sba.gov
202-205-7173

6) Who is the Reviewing Official? (According to OMB, this the agency IO or other agency head designee who is other than the official procuring the system or the official who conducts the PIA).

Christine Liu
Chief Information Officer/Chief Privacy Officer
Office of the Chief Information Officer
Christine.Liu@sba.gov
202-205-6708

B. PIA PROCESS APPLICATION/GENERAL INFORMATION:

1) Does this system contain any information about individuals?

Yes

a. Is this information identifiable to the individual!?

Yes

b. Is the information about individual members of the public?'

Yes

c. Is the information about employees?

No

2) What is the purpose of the LAS System?

The system is a database of SBA loans, including guaranteed business loans 7(a) and 503/504, microloans to intermediaries, and disaster business and home loans, enabling the Agency to track payments, servicing, liquidation, litigation and accounting actions on the individual loans and includes the following subsystems:

- Credit Bureau Reporting,
- Delinquent Loan Collection System,
- Field Cashiering System
- General Ledger Only
- IRS 1099C System,
- Loan Litigation & Liquidation Tracking System,
- Microloan Mainframe,
- Preauthorized Debit System, and
- Treasury Offset System

3) What legal authority authorizes the purchase or development of this System/Application?

15 U.S.C. § 634(b)(6), 44 U.S.C. § 3101. Public Law 85-536, 15 U.S.C. § 631 et seq. (Small Business Act, all provisions relating to loan programs); 44 U.S.C. § 3101 (Records Management by Federal Agencies); and Public Law 103-62 (Government Performance and Results Act). Public Law 85-699 as amended 15 U.S.C. § 661 et seq. (Small Business Investment Act of 1958, all provisions relating to loan programs)

C. DATA IN THE PROCESS

1) What categories of individuals are covered in the system?

Borrowers, Principals of Borrowers, Guarantors of Borrowers, Lending Partner, Financial, address, personal identifier (SSN) and demographic

2) What are the sources of the information in the system?

a. Is the source of the information from the individual or is it taken from another source? If not directly from the individual, source then what other source

Lending Partners, SBAREF, Loan Application Tracking System, DCMS, Electronic lending system

b. What Federal agencies are providing data for use in the process?

None

c. What State and local agencies are providing data for use in the process?

None

d. From what other third party sources will data be collected?

All Credit Reporting Agencies

e. What information will be collected from the employee and the public?

The information in the system is derived from other SBA systems. Etran, LATs, ALCS, DCMS, the 7(a), 503, 504 Servicing System, All information about individuals is collected through those systems, this system is the database which holds all the information collected through the other systems. This data includes social security numbers (SSN), names, addresses and phone numbers.

3) Accuracy, Timeliness, and Reliability

a. How will data collected from sources other than SBA records be verified for accuracy?

Credit Reporting Agencies provide only outside data, they are the original source

b. How will data be checked for completeness?

Original Source

c. Is the Data Current? What steps or procedures are taken to ensure the data is current and not out-of date? Name the document (e.g., data models)

Data is current according to Credit Reporting Agencies' records

d. Are the data elements described in detail and documented? If Yes, What is the name of the document?

SOP 20 03 3 – Accounting Structure

D. ATTRIBUTES OF THE DATA

1) Is the use of the data both relevant and necessary to the purpose for which the process is being designed?

Yes, data is used to verify SBA program compliance and record specifics of loans

2) Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?

No

3) Will the new data be placed in the individual's record?

No

4) Can the system make determinations about employees/public that would not be possible without the new data?

No

5) How will the new data be verified for relevance and accuracy?

N/A

6) If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?

Agency Security Access Procedures – Data access is limited to those individuals with authorized use and only for specific screens as they pertain to the user's role/need.

7) If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access through the process? Explain.

Agency Security Roles and Procedures/Controls – Agency Security Access Procedures – Access is limited by control assignment of a responsibility profile to all users. Each responsibility comes with a pre-determined set of privileges, limiting data that may be viewed to those screens and reports that are within the duties and needs of the user

8) How will the data be retrieved? Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.

Data can be retrieved by personal identifier (SSN), individual name, business name, employer identifier, loan number

9) What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?

Reports can be produced on individual's records to respond to inquiries which comply with FOIA and Privacy Act requirements. Access is restricted to Program Officials with the "need to know" and to public inquiries where the specific data complies with FOIA and Privacy Act guidelines.

10) What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary), or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent?

Individuals can decline to provide some demographic information requested. Information such as veteran status, gender, race, and ethnicity of an individual are not required.

E. MAINTENANCE AND ADMINISTRATIVE CONTROLS

1) If the information in the process operated in more than one site, how will consistent use of the data be maintained in all sites?

System operated on one site only

2) What are the retention periods of data in the system?

As delineated in SBA's Privacy Act Systems of Records, SBA 20 and SBA 21, In accordance with SBA Standard Operating Procedure 00 41 2, Item Nos. 50:04, 50:08, 50:09, 50:10, 50:11, 50:12, 50:13, 50:19, 50:22, 55:02, 70:09, 70:13, and appendices 17, 18 and 21.

3) What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?

As delineated in SBA's Privacy Act Systems of Records, SBA 20 and SBA 21, In accordance with SBA Standard Operating Procedure 00 41 2, Item Nos. 50:04, 50:08, 50:09, 50:10, 50:11, 50:12, 50:13, 50:19, 50:22, 55:02, 70:09, 70:13, and appendices 17, 18 and 21.

4) Are the systems in the process using technologies in ways that the SBA has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?

NO

5) How does the use of this technology affect public/employee privacy?

The System does not currently generate reports specific to individuals or individual loans. Reports can be produced on individual's records for the purpose of workload management and inquiries which comply with FOIA and Privacy Act requirements. Access is restricted to Program Officials with the "need to know" and to public inquiries where the specific data complies with FOIA and Privacy Act guidelines.

6) Will this system in the process provide the capability to identify, locate, and monitor individuals? If yes, explain

No the system cannot identify, locate or monitor individuals. It can retrieve information by personal identifier and by name, however, only that information that is already in the system, and only by those who have been granted access to the system and then only specific to their role with SBA.

The system does not currently generate reports specific to individuals or individual loans. Reports can be produced on individual's records for the purpose of workload management and inquiries which comply with FOIA and Privacy Act requirements. Access is restricted to Program Officials with the "need to know" and to public inquiries where the specific data complies with FOIA and Privacy Act guidelines.

7) What kinds of information are collected as a function of the monitoring of individuals?

We do not monitor individuals, we monitor loans, and therefore this is not applicable.

8) What controls will be used to prevent unauthorized monitoring?

Agency Security Roles and Procedures/Controls – Agency Security Access

Procedures – Access is limited by controlled assignment of a responsibility profile to all users. Each responsibility comes with a pre-determined set of privileges, limiting data that may be viewed to those screens and reports that are within the duties and needs of the user

9) Under which Privacy Act systems of records notice does the system operate? Provide number and name.

SBA's Privacy Act Systems of Records, SBA 20 and SBA 21

10) If the system is being modified, will the Privacy Act Systems of records notice require amendment or revision? Explain.

NA

F. ACCESS TO DATA:

1) Who will have access to the data in the System? (E.g. contractors, users, managers, system administrators, developers, tribes, other)

Contractors, users, managers, system administrators, developers

2) How is access to the data by a user determined? Are criteria, procedures, controls and responsibilities regarding access documented?

Criteria – Agency Security Roles and Procedures/Controls – Agency Security Access Procedures – Access is limited by controlled assignment of a responsibility profile to all users. Each responsibility comes with a pre-determined set of privileges, limiting data that may be viewed to those screens and reports that are within the duties and needs of the user.

3) Will users have access to all data on the system or will the user's access be restricted? Explain

Access is limited by controlled assignment of a responsibility profile to all users. Each responsibility comes with a pre-determined set of privileges, limiting data that may be viewed to those screens and reports that are within the duties and needs of the user.

4) What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access?

Agency Security Roles and Procedures/Controls – Agency Security Access Procedures – Access is limited by controlled assignment of a responsibility profile to all users. Each responsibility comes with a pre-determined set of privileges, limiting data that may be viewed to those screens and reports that are within the

duties and needs of the user.

Education of Agency and contractor staff regarding the Privacy Act rules and prohibitions on the dissemination or use of non-public information is mandatory and ongoing. System audit trails can be used to document suspicious or irregular logon and navigation of the system. Agency network log-on procedures mandate a posted Privacy notice be viewed and acknowledged prior to entry. SBA Privacy Act Systems of Records SBA 20 and SBA 21 define routine uses of this information and serve as a control by defining acceptable uses. Limiting access to sensitive financial information to only those with a need to know remains the best and primary control.

- 5) Are contractors involved with the design and development of the: system and will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?**

Yes, contract clauses are inserted in their contracts and other regulatory measures addressed

- 6) Do other systems share data or have access to the data in the system? If yes, explain.**

Data is downloaded to other databases; however, there is no direct interface with other systems.

- 7) Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**

Office of the Chief Information Officer

- 8) Will other agencies share data or have access to the data in this: system?**

NO

- 9) How will the data be used by the other agency?**

NA

- 10) Who is responsible for assuring proper use of the data?**

NA

G. PRIVACY IMPACT ANALYSIS

1) Discuss what privacy risks were identified and how they were mitigated for types of information collected.

Because the system collects some PII information and not everyone needs to have access to the information, only those that need to know the EIN or SSN information will be able to view it. Also only those need to query based on EIN or SSN have permission to do so.

2) Describe any types of controls that may be in place to ensure that information is used as intent.

Users have to sign rules of behavior document. SBA will pre-determine roles for users in the system which means that specific forms will be made available to a user depending on their job function at the SBA.

3) Discuss what privacy risks were identified and how they were mitigated for information shared internal and external?

The system uses extracts. Only required data is exchanged. Electronic data is transferred using a secure interface including, VPN, secure lease line, file encryption, secure shell and secure FTP.

A user's access is based on the responsibility assigned to the user. Therefore, users' access is restricted by responsibility. The pre-determined responsibilities-as described in the question above -assign different forms and types of data to a user.

4) What privacy risks were identified and describe how they were mitigated for security and access controls?

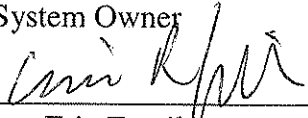
To ensure employees do not view PII data not required in the performance of their jobs, user accounts are assigned specific roles and responsibilities. Users are limited in their access to areas of the system appropriate for those responsibilities.

Privacy Impact Assessment for LAS

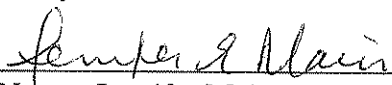
Responsible Officials - Approval Signature Page

The Following Officials Have Approved This Document:


1) System Owner

 (Signature) 10/2/08 (Date)
Name: Eric Zarnikow
Title: Associate Administrator, Office of Capital Access


2) System Owner

 (Signature) 10/1/08 (Date)
Name: Jennifer Main
Title: Chief Financial Officer

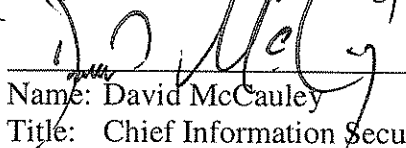
3) System Owner

 (Signature) 10/2/08 (Date)
Name: Herbert L. Mitchell
Title: Associate Administrator, Office of Disaster Assistance

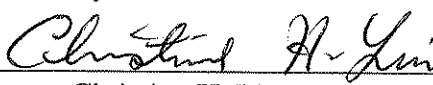
4) System Program/Project Manager

 (Signature) 10/2/08 (Date)
Name: Stephen Kucharski
Title: Modernization Program Manager

5) System IT Security Manager

 (Signature) 10/27/08 (Date)
Name: David McCauley
Title: Chief Information Security Officer

6) Privacy Official

 (Signature) 11/3/08 (Date)
Name: Christine H. Liu
Title: Chief Information Officer/Chief Privacy Officer